



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

BCF to

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/259,620	02/26/1999	JAMES Q. MI	INTL-0160-US	5503

7590 03/18/2002

TIMOTHY N. TROP
TROP, PRUNER, HU & MILES
8554 KATY FREEWAY
SUITE 100
HOUSTON, TX 77024

EXAMINER

MEISLAHN, DOUGLAS J

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 03/18/2002

3

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/259,620

Applicant(s)

MI ET AL.

Examiner

Douglas J. Meislahn

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☐ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☐ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on ____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 6-9 and 16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
3. Claim 6 recites the limitation "the first computer system" in lines 3-4 and "said another computer system" in lines 5-6. There are insufficient antecedent bases for these limitations in the claim.
4. Claim 16 recites the limitation "the algorithmic unit" in line 2 and "the registers" in line 2. There are insufficient antecedent bases for these limitations in the claim.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1, 5, 6, 10, 11, 13, 15, 16, and 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zdepski et al. (5825884) in view of Schneier (*Applied Cryptography*).

In lines 64-67 of column 4, Zdepski et al. talk about encrypting a platform's identifier with a recipient's public key. In the following column, this cryptogram is sent to

the recipient. These disclosures clearly meet the limitations of the last three clauses of the first claim. Zdepski et al. do not explicitly say that a request for identification originates at the eventual recipient and is relayed to the platform. In the most simple authentication protocol using public keys, a host sends a recipient a random string (Schneier – pages 53-54). The recipient responds with an identifier and a cryptogram of the random string. Hence the act of sending the random string is a request for identification. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made for the transaction server in Zdepski et al. to request an identifier from the subscriber platform as a way to authenticate the subscriber, as taught by Schneier.

With respect to claim 5, Zdepski et al. are using a public key, which would be associated with a user or address. As the content is requested, this user can be seen as a web site. Regarding claims 18-20, public key algorithms are collision-resistant, non-commutative, and one-way.

In regard to claims 10, 11, and 13, on pages 185-186, Schneier teaches certificates as a means to “thwart attempts to substitute one key for another”. This is a type of verification. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to verify the public key used in Zdepski et al. to avoid undesired key swaps as taught by Schneier.

7. Claims 2, 3, 7, 8, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zdepski et al. and Schneier in view of Dwork et al. (5978482).

Zdepski et al. show sending identifiers encrypted with a recipient's public key. They do not say that the identifiers are processor numbers. In figure 6 and line 8-10 of column 13, Dwork et al. use processor numbers as a way to uniquely identify users. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use a processor number, as taught by Dwork et al., for the identifier in Zdepski et al. to uniquely identify the sender.

8. Claims 4 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zdepski et al. and Schneier.

Zdepski et al. show sending identifiers encrypted with a recipient's public key. They do not say that the public key had been sent from the recipient to the encrypting entity. Official notice is taken that it is old and well known for an entity to send its public key to a recipient so that the recipient can encrypt data that can then only be decrypted by the public key's originator. This also saves the encrypting entity from searching for the public key. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to send the public key from the transaction server to the subscriber platform, thereby saving the subscriber platform from searching for the key.

9. Claims 5 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier and Zdepski et al. as applied to claims 1 and 11 above, and further in view of Linehan (6327578).

Zdepski et al. and Schneier show sending identifiers encrypted with a recipient's verified public key. They do not say that the key indicates an URL address. In lines 14-

Art Unit: 2132

20 of column 5, Linehan teaches including an URL in a certificate. Thus the public key would indicate an URL address. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to follow Linehan's example and include an URL address in the certificate of Schneier associated with the public key in Zdepski et al. This ties the key to a specific entity.

10. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Zdepski et al. and Schneier as applied to claim 10 above, and further in view of Dwork et al.

Zdepski et al. and Schneier show sending identifiers encrypted with a recipient's verified public key. They do not say that the identifier is a processor number. In figure 6 and line 8-10 of column 13, Dwork et al. use processor numbers as a way to uniquely identify users. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use a processor number, as taught by Dwork et al., for the identifier in Zdepski et al. to uniquely identify the sender.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Berger et al. (5850446), Uyehara et al. (6154214), Takahashi et al. (6195432), Challenger et al. (6081793), Ho (6148342), Shieh (5424727), Nawaz et al. (5959621), Shimakawa et al. and (6055536).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.



DJM
March 12, 2002

Douglas J. Meislahn
Examiner
Art Unit 2132



GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100